

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Ryogo YANAGISAWA :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed March 26, 2004 : Attorney Docket No. 2004_0472A

PUBLIC KEY GENERATION APPARATUS, :
SHARED KEY GENERATION APPARATUS,
KEY EXCHANGE APPARATUS, AND KEY :
EXCHANGING METHOD

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

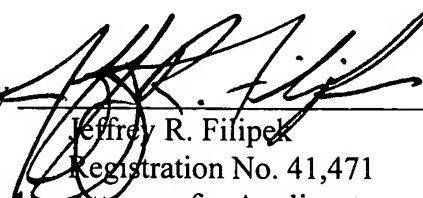
Applicant in the above-entitled application hereby claims the date of priority under the International Convention of Japanese Patent Application No. 2003-088788, filed March 27, 2003, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Ryogo YANAGISAWA

By



Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicant

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
March 26, 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月27日
Date of Application:

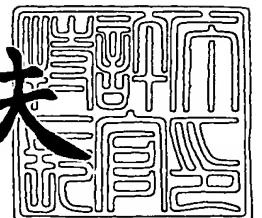
出願番号 特願2003-088788
Application Number:
[ST. 10/C]: [JP 2003-088788]

出願人 松下電器産業株式会社
Applicant(s):

2003年 7月22日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3058017

【書類名】 特許願

【整理番号】 2037840200

【提出日】 平成15年 3月27日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 柳澤 玲互

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100081813

【弁理士】

【氏名又は名称】 早瀬 憲一

【電話番号】 06(6395)3251

【手数料の表示】

【予納台帳番号】 013527

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9600402

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵生成装置、共有鍵生成装置、鍵交換装置、及び鍵交換方法

【特許請求の範囲】

【請求項 1】 乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし、 $0 < k < q$ となる乱数 k を生成する乱数生成手段と、

前記乱数 k と、前記元 g と、前記素数 q より、公開鍵 y を前記有限群 F 上で演算し出力する公開鍵生成手段とを備え、

少なくとも前記乱数生成手段と前記公開鍵生成手段とが同一の半導体集積回路上に集積され、

公開鍵配布元となる第 1 のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y を取得し、該公開鍵 y を公開鍵配布先となる第 2 のユーザーへ伝送する、

ことを特徴とする公開鍵生成装置。

【請求項 2】 請求項 1 記載の公開鍵生成装置において、

前記公開鍵生成手段は、

前記乱数 k と、前記元 g と、前記素数 q より、前記公開鍵 y を、

$$y = g^k \bmod q$$

として、前記有限群 F 上で演算し出力する、

ことを特徴とする公開鍵生成装置。

【請求項 3】 請求項 1 記載の公開鍵生成装置において、

前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、

前記公開鍵生成手段が、前記乱数 k と、前記元 G と、前記素数 q より、前記公開鍵 y を、

$$y = kG \bmod q$$

として、前記楕円曲線 $E(F)$ 上で演算し出力する、

ことを特徴とする公開鍵生成装置。

【請求項 4】 請求項 1 ないし 3 のいずれかに記載の公開鍵生成装置におい

て、

前記乱数生成手段が、前記公開鍵 y_a の演算終了後に、新たな乱数を生成する、

ことを特徴とする公開鍵生成装置。

【請求項 5】 乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、

共有鍵配布先となる第 2 のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記乱数 k_a より、共有鍵 K_a を前記有限群 F 上で演算し出力する共有鍵生成手段とを備え、

少なくとも前記乱数生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、

共有鍵配布元となる第 1 のユーザーの制御手段が、前記共有鍵配布先となる第 2 のユーザーより前記公開鍵 y_b を取得し、前記乱数生成手段と前記共有鍵生成手段とを制御して、前記共有鍵 K_a を導出する、

ことを特徴とする共有鍵生成装置。

【請求項 6】 請求項 5 記載の共有鍵生成装置において、

前記共有鍵生成手段は、

前記共有鍵配布先となる第 2 のユーザーが生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、

$$K_a = y_b^{k_a} \bmod q$$

として、前記有限群 F 上で演算し出力する、

ことを特徴とする共有鍵生成装置。

【請求項 7】 請求項 5 記載の共有鍵生成装置において、

前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、

前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、

$$K_a = k_a y_b \bmod q$$

として、前記楕円曲線 E (F) 上で演算し出力する、
ことを特徴とする共有鍵生成装置。

【請求項 8】 請求項 5 ないし 7 のいずれかに記載の共有鍵生成装置において、

前記乱数生成手段は、前記共有鍵 K_a の演算終了後に、新たな乱数を生成する
ことを特徴とする共有鍵生成装置。

【請求項 9】 乗算が定義された有限群 F 上の元を g 、前記 g の素数である
位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、

前記乱数 k_a と、前記元 g と、前記素数 q より、公開鍵 y_a を前記有限群 F 上
で演算し出力する公開鍵生成手段と、

共有鍵配布先となる第 2 のユーザーが発生した $0 < k_b < q$ となる乱数 k_b よ
り生成された公開鍵 y_b と、前記乱数 k_a より、共有鍵 K_a を前記有限群 F 上で
演算し出力する共有鍵生成手段とを備え、

少なくとも前記乱数生成手段と前記公開鍵生成手段と前記共有鍵生成手段とが
同一の半導体集積回路上に集積され、

共有鍵配布元となる第 1 のユーザーの制御手段が、前記乱数生成手段と前記公
開鍵生成手段とを制御して前記公開鍵 y_b を取得し、前記共有鍵生成手段を制御
して前記共有鍵 K_a を導出する、

ことを特徴とする鍵交換装置。

【請求項 10】 請求項 9 記載の鍵交換装置において、

前記公開鍵生成手段は、前記乱数 k_a と、前記元 g と、前記素数 q より、前記
公開鍵 y_a を $y_a = g^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力
し、

前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが、前記乱数
 k_b より前記有限群 F 上で演算し生成した前記公開鍵 $y_b = g^{k_b} \bmod q$
と、前記乱数 k_a により、前記共有鍵 K_a を $K_a = y_b^{k_a} \bmod q$ と
して、前記有限群 F 上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項 11】 請求項 9 記載の鍵交換装置において、

前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、

前記公開鍵生成手段は、前記乱数 k_a と、前記元 G と、前記素数 q より、前記公開鍵 y_a を、 $y_a = k_a G \pmod{q}$

として、前記楕円曲線 $E(F)$ 上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが、前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \pmod{q}$ と、前記乱数 k_a により、前記共有鍵 K_a を、

$K_a = k_a y_b \pmod{q}$

として、前記楕円曲線 $E(F)$ 上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項 12】 請求項 9 ないし 11 のいずれかに記載の鍵交換装置において、

前記乱数生成手段は、前記公開鍵 y_a と前記共有鍵 K_a の演算がともに終了した後に、新たな乱数を生成する、

ことを特徴とする鍵交換装置。

【請求項 13】 乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、

前記乱数 k_a を一時的に記憶する秘密鍵保持手段と、

前記乱数 k_a と、前記元 g と、前記素数 q より、公開鍵 y_a を前記有限群 F 上で演算し出力する公開鍵生成手段と、

共有鍵配布先となる第 2 のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記秘密鍵保持手段が保持する乱数 k_a により、共有鍵 K_a を前記有限群 F 上で演算し出力する共有鍵生成手段とを備え、

少なくとも、前記乱数生成手段と、前記秘密鍵保持手段と、前記公開鍵生成手段と、前記共有鍵生成手段とが、同一の半導体集積回路上に集積され、

共有鍵配布元となる第 1 のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y_a を取得して、該公開鍵 y_a を前記共有

鍵配布先となる第2のユーザーへ伝送し、

前記共有鍵配布先となる第2のユーザーより前記公開鍵 y_b を取得して、前記共有鍵生成手段を制御して前記共有鍵 K_a を導出する、

ことを特徴とする鍵交換装置。

【請求項14】 請求項13記載の鍵交換装置において、

前記公開鍵生成手段は、前記乱数 k_a と、前記元 g と、前記素数 q より前記公開鍵 y_a を、

$$y_a = g^{k_a} \bmod q$$

として、前記有限群 F 上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが前記乱数 k_b より前記有限群 F 上で演算し生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と、前記秘密鍵保持手段が記憶している乱数 k_a より、前記共有鍵 K_a を、

$$K_a = y_b^{k_a} \bmod q$$

として、前記有限群 F 上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項15】 請求項13記載の鍵交換装置において、

前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記公開鍵生成手段は、前記乱数 k_a と、前記元 G と、前記素数 q より、前記公開鍵 y_a を、

$$y_a = k_a G \bmod q$$

として、前記楕円曲線 $E(F)$ 上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが、前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \bmod q$ と、前記秘密鍵保持手段が記憶している乱数 k_a により、前記共有鍵 K_a を、

$$K_a = k_a y_b \bmod q$$

として、前記楕円曲線 $E(F)$ 上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項16】 請求項13ないし15のいずれかに記載の鍵交換装置にお

いて、

前記乱数生成手段は、前記公開鍵 y_a の演算終了後に、新たな乱数を生成する

ことを特徴とする鍵交換装置。

【請求項 17】 請求項 13 ないし 15 のいずれかに記載の鍵交換装置において、

前記乱数生成手段は、前記共有鍵 K_a の演算終了後に、新たな乱数を生成し、

前記秘密鍵保持手段が、前記乱数生成手段の生成した前記新たな乱数を保持する、

ことを特徴とする鍵交換装置。

【請求項 18】 請求項 9 ないし 17 のいずれかに記載の鍵交換装置を使用し、鍵を共有したいユーザーの双方が前記鍵を共有する、

ことを特徴とする鍵交換方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、公開されたネットワークにおける電子情報の伝送を第三者に秘匿し、安全に行うために用いられる公開鍵生成装置、共有鍵生成装置、鍵交換装置及び鍵交換方法に関し、特に第三者による装置の流用あるいは改変が極めて困難な公開鍵生成装置、共有鍵生成装置、鍵交換装置及び鍵交換方法を提供するものである。

【0002】

【従来の技術】

従来の有限群上の離散対数問題を利用した鍵交換装置として、Diffie-Hellman 鍵交換装置（以下、DH 鍵交換装置と呼ぶ）が知られている（例えば、特許文献 1 参照）。

【0003】

図 5 に、DH 鍵交換装置の従来例を示す。図 5 において、51 は公開鍵配布元となるユーザー 1 の乱数生成手段、52 はユーザー 1 の公開鍵生成手段、53 は

ユーザー 1 の共有鍵生成手段である。また、54 はユーザー 2 の乱数生成手段、55 は公開鍵配布先となるユーザー 2 の公開鍵生成手段、56 はユーザー 2 の共有鍵生成手段である。

【0004】

以下、図 5 を用いて、ユーザー 1 の従来の DH 鍵交換装置とユーザー 2 の従来の DH 鍵交換装置とで、ユーザー 1 とユーザー 2 とが鍵を共有する方法について説明する。

【0005】

有限群 F 上では乗算が定義されているものとする。有限群 F 上の元を g (g は素数である位数 q を持つもの) とする。また、有限群 F 、元 g 、素数 q は公開されており、少なくともユーザー 1 とユーザー 2 との間で共有されているものとする。ユーザー 1 とユーザー 2 は以下のステップを経て、鍵を共有する。

【0006】

(ステップ 1)

ユーザー 1 は乱数生成手段 51 を用いて乱数 k_a ($0 < k_a < q$) を生成し、これをユーザー 1 の秘密鍵 k_a とする。同様にユーザー 2 は乱数生成手段 54 を用いて乱数 k_b ($0 < k_b < q$) を生成し、これをユーザー 2 の秘密鍵 k_b とする。

【0007】

(ステップ 2)

ユーザー 1 は公開鍵生成手段 52 を用いて公開鍵 y_a を生成する。ここで $y_a = g^{k_a} \bmod q \cdots$ (数 1) であり、 y_a は有限群 F 上で演算され求められる。 $\bmod q$ は q で割った余りを示す。同様にユーザー 2 は公開鍵生成手段 55 を用いて公開鍵 y_b を生成する。ここで、

$y_b = g^{k_b} \bmod q \cdots$ (数 2)

であり、 y_b は有限群 F 上で演算され求められる。

【0008】

(ステップ 3)

ユーザー 1 はユーザー 2 へ公開鍵 y_a を伝送し、ユーザー 2 はユーザー 1 へ公開鍵 y_b を伝送する。すなわち、ユーザー 1 とユーザー 2 との間で公開鍵 y_a 、公開鍵 y_b を交換する。

【0009】

(ステップ 4).

ユーザー 1 は共有鍵生成手段 53 を用いて鍵 K_a を生成する。ここで、

$$\begin{aligned} K_a &= y_b^{k_a} \bmod q \\ &= g^{(k_a \times k_b)} \bmod q \quad \cdots (\text{数 } 3) \end{aligned}$$

であり、 K_a は有限群 F 上で演算され求められる。同様にユーザー 2 は共有鍵生成手段 56 を用いて鍵 K_b を生成する。ここで、

$$\begin{aligned} K_b &= y_a^{k_b} \bmod q \\ &= g^{(k_a \times k_b)} \bmod q \quad \cdots (\text{数 } 4) \end{aligned}$$

であり、 K_b は有限群 F 上で演算され求められる。

【0010】

以上のステップ 1 ~ 4 により、ユーザー 1 とユーザー 2 との間で同一の共有鍵 $K = K_a = K_b$ が生成される。

【0011】

上記の DH 鍵交換装置では、有限群 F における離散対数問題の解法の困難性に基づいて装置が構成されている。すなわち $y = g^x \bmod q$ ($0 < x < q$) を満たす整数 x を y 、 g より求める困難性を安全性の根拠としている。

【0012】

有限群 F における離散対数問題の解法の困難性を根拠とする暗号系として、楕円曲線暗号系が広く知られている。すなわち、有限体上の楕円曲線を $E(F)$ 、楕円曲線 $E(F)$ 上のあらかじめユーザー 1 とユーザー 2 との間で共有されている点を G とし、楕円曲線 $E(F)$ 上の点 x との演算 xG が定義されているものとする、数 1 ~ 数 4 はそれぞれ数 5 ~ 数 8 に書き改めることができる。

【0013】

$$y_a = k_a G \bmod q \quad \cdots (\text{数 } 5)$$

$$y_b = k_b G \bmod q \quad \cdots (\text{数 } 6)$$

$$\begin{aligned} K_a &= k_a(yb) \bmod q \\ &= k_a k_b G \bmod q \quad \cdots (\text{数7}) \end{aligned}$$

$$\begin{aligned} K_b &= k_b(ya) \bmod q \\ &= k_a k_b G \bmod q \quad \cdots (\text{数8}) \end{aligned}$$

【0014】

以上のように、楕円曲線暗号系を使用しても、ユーザー1とユーザー2との間で同一の共有鍵 $K = K_a = K_b$ が生成される。素数 q を160ビット程度に選べば、現在知られている最も効率のよい計算アルゴリズムを使用し、最新のコンピュータを用いても、現実的な時間で解は求めることができないことが知られている。

【0015】

上述したように、DH鍵交換装置では g^x (楕円曲線暗号系における xG) が鍵交換における主要な演算処理である。通常秘密鍵 x は素数 q と同程度のビット長 (楕円曲線暗号系では160ビット程度) にとられるが、ユーザー1、ユーザー2以外の悪意ある第3者が g^x (あるいは xG) を流用、あるいは鍵長をより長く改変するようなことがあれば、より強固な公開鍵暗号系を容易に構成することも可能であり、暗号系の保安上好ましくなく、特に主要な演算に高速演算アルゴリズムを使用している場合、さらに被害は甚大なものとなる。

【0016】

【特許文献1】

特開2001-352319号公報 (第9頁、図4)

【0017】

【発明が解決しようとする課題】

従来の公開鍵生成装置、共有鍵生成装置、鍵交換装置、及び鍵交換方法は以上のように構成されており、第3者からの攻撃に対しなんら配慮されないDH鍵交換装置が用いられており、万が一主要な演算を悪意ある第3者が流用、あるいは改変することがあれば、国家の安全保障上極めて甚大な被害をもたらすという問題点を有していた。

【0018】

本発明は以上のような問題点を解消するためになされたもので、第3者による装置の流用、あるいは改変が極めて困難な公開鍵生成装置、共有鍵生成装置、鍵交換装置、及び鍵交換方法を提供することを目的とする。

【0019】

【課題を解決するための手段】

上記課題を解決するために、本発明（請求項1）にかかる公開鍵生成装置は、乗算が定義された有限群F上の元をg、前記gの素数である位数をqとし、 $0 < k a < q$ となる乱数kaを生成する乱数生成手段と、前記乱数kaと、前記元gと、前記素数qより、公開鍵yaを前記有限群F上で演算し出力する公開鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段とが同一の半導体集積回路上に集積され、公開鍵配布元となる第1のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵yaを取得し、該公開鍵yaを公開鍵配布先となる第2のユーザーへ伝送するものである。

【0020】

また、本発明（請求項2）にかかる公開鍵生成装置は、請求項1記載の公開鍵生成装置において、前記公開鍵生成手段は、前記乱数kaと、前記元gと、前記素数qより、前記公開鍵yaを、 $y a = g^{k a} \bmod q$ として、前記有限群F上で演算し出力するものである。

【0021】

また、本発明（請求項3）にかかる公開鍵生成装置は、請求項1記載の公開鍵生成装置において、前記有限群Fを有限体上の楕円曲線E（F）とし、前記楕円曲線E（F）の元をGとし、前記公開鍵生成手段が、前記乱数kaと、前記元Gと、前記素数qより、前記公開鍵yaを、 $y a = k a G \bmod q$ として、前記楕円曲線E（F）上で演算し出力するものである。

【0022】

また、本発明（請求項4）にかかる公開鍵生成装置は、請求項1ないし3のいずれかに記載の公開鍵生成装置において、前記乱数生成手段が、前記公開鍵yaの演算終了後に、新たな乱数を生成するものである。

【0023】

また、本発明（請求項5）にかかる共有鍵生成装置は、乗算が定義された有限群F上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、共有鍵配布先となる第2のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記乱数 k_a より、共有鍵 K_a を前記有限群F上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第1のユーザーの制御手段が、前記共有鍵配布先となる第2のユーザーより前記公開鍵 y_b を取得し、前記乱数生成手段と前記共有鍵生成手段とを制御して、前記共有鍵 K_a を導出するものである。

【0024】

また、本発明（請求項6）にかかる共有鍵生成装置は、請求項5記載の共有鍵生成装置において、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、 $K_a = y_b^{k_a} \bmod q$ として、前記有限群F上で演算し出力するものである。

【0025】

また、本発明（請求項7）にかかる共有鍵生成装置は、請求項5記載の共有鍵生成装置において、前記有限群Fを有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、 $K_a = k_a y_b \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力するものである。

【0026】

また、本発明（請求項8）にかかる共有鍵生成装置は、請求項5ないし7のいずれかに記載の共有鍵生成装置において、前記乱数生成手段は、前記共有鍵 K_a の演算終了後に、新たな乱数を生成するものである。

【0027】

また、本発明（請求項9）にかかる鍵交換装置は、が定義された有限群F上の

元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、前記乱数 k_a と、前記元 g と、前記素数 q より、公開鍵 y_a を前記有限群 F 上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第 2 のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記乱数 k_a より、共有鍵 K_a を前記有限群 F 上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第 1 のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y_b を取得し、前記共有鍵生成手段を制御して前記共有鍵 K_a を導出するものである。

【0028】

また、本発明（請求項 10）にかかる鍵交換装置は、請求項 9 記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数 k_a と、前記元 g と、前記素数 q より、前記公開鍵 y_a を $y_a = g^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが、前記乱数 k_b より前記有限群 F 上で演算し生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を $K_a = y_b^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力するものである。

【0029】

また、本発明（請求項 11）にかかる鍵交換装置は、請求項 9 記載の鍵交換装置において、前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記公開鍵生成手段は、前記乱数 k_a と、前記元 G と、前記素数 q より、前記公開鍵 y_a を、 $y_a = k_a G \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが、前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、 $K_a = k_a y_b \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力するものである。

【0030】

また、本発明（請求項 12）にかかる鍵交換装置は、請求項 9 ないし 11 のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵 y_a と前記共有鍵 K_a の演算がともに終了した後に、新たな乱数を生成するものである。

【0031】

また、本発明（請求項 13）にかかる鍵交換装置は、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、前記乱数 k_a を一時的に記憶する秘密鍵保持手段と、前記乱数 k_a と、前記元 g と、前記素数 q より、公開鍵 y_a を前記有限群 F 上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第 2 のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記秘密鍵保持手段が保持する乱数 k_a により、共有鍵 K_a を前記有限群 F 上で演算し出力する共有鍵生成手段とを備え、少なくとも、前記乱数生成手段と、前記秘密鍵保持手段と、前記公開鍵生成手段と、前記共有鍵生成手段とが、同一の半導体集積回路上に集積され、共有鍵配布元となる第 1 のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y_a を取得して、該公開鍵 y_a を前記共有鍵配布先となる第 2 のユーザーへ伝送し、前記共有鍵配布先となる第 2 のユーザーより前記公開鍵 y_b を取得して、前記共有鍵生成手段を制御して前記共有鍵 K_a を導出するものである。

【0032】

また、本発明（請求項 14）にかかる鍵交換装置は、請求項 13 記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数 k_a と、前記元 g と、前記素数 q より前記公開鍵 y_a を、 $y_a = g^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが前記乱数 k_b より前記有限群 F 上で演算し生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と、前記秘密鍵保持手段が記憶している乱数 k_a より、前記共有鍵 K_a を、 $K_a = y_b^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力するものである。

【0033】

また、本発明（請求項 15）にかかる鍵交換装置は、請求項 13 記載の鍵交換

装置において、前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記公開鍵生成手段は、前記乱数 k_a と、前記元 G と、前記素数 q より、前記公開鍵 y_a を、 $y_a = k_a G \pmod{q}$ として、前記楕円曲線 $E(F)$ 上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが、前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \pmod{q}$ と、前記秘密鍵保持手段が記憶している乱数 k_a により、前記共有鍵 K_a を、 $K_a = k_a y_b \pmod{q}$ として、前記楕円曲線 $E(F)$ 上で演算し出力するものである。

【0034】

また、本発明（請求項16）にかかる鍵交換装置は、請求項13ないし15のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵 y_a の演算終了後に、新たな乱数を生成するものである。

【0035】

また、本発明（請求項17）にかかる鍵交換装置は、請求項13ないし15のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記共有鍵 K_a の演算終了後に、新たな乱数を生成し、前記秘密鍵保持手段が、前記乱数生成手段の生成した前記新たな乱数を保持するものである。

【0036】

また、本発明（請求項18）にかかる鍵交換装置は、請求項9ないし17のいずれかに記載の鍵交換装置を使用し、鍵を共有したいユーザーの双方が前記鍵を共有するものである。

【0037】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

【0038】

（実施の形態1）

図1は、本発明の請求項1に対応する実施の形態1による公開鍵生成装置のブロック構成図を示すものである。

【0039】

図1において、11は乱数生成手段、12は公開鍵生成手段、13は1つのパッケージに収められた半導体集積回路（以下LSIと呼ぶ）、14は半導体集積回路（LSI）13を制御する制御手段、15は半導体集積回路13、制御手段14を含む公開鍵配布元であるユーザー1の公開鍵生成装置である。

【0040】

以下、図1を参照しながら、本実施の形態1の公開鍵生成装置の動作について説明する。

乱数生成手段11は、制御手段14によって制御され、乱数 k_a を生成し、これを秘密鍵 k_a とする。ここで秘密鍵 k_a は、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とした時、 $0 < k_a < q$ を満たしている。制御手段14は、乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段14には、例えばマイクロコンピュータが使用される。

【0041】

公開鍵生成手段12は、上記制御手段14により制御され、公開鍵 y_a を生成する。公開鍵 y_a は、上述した数1式に基づいて秘密鍵 k_a より求められる。生成された公開鍵 y_a は、制御手段14によって公開鍵配布先であるユーザー2へ伝送される。

【0042】

少なくとも乱数生成手段11と、公開鍵生成手段12を、LSI13内部に集積すれば、上記数1式の演算を他の暗号処理へ流用、あるいは改変することは非常に困難である。加えて制御手段14を集積すれば、さらに効果が高まる。また公開鍵 y_a 生成後、乱数生成手段11が、新たに乱数を生成するようにすれば、公開鍵 y_a は出力される毎に異なる値をとる。この時、上記数1式から明らかのように、公開鍵 y_a は、乱数の関数となる。よって、ユーザー1を含めた誰もが、本公開鍵生成装置15を公開鍵 y_a の生成以外に流用、あるいは改変することは極めて困難である。

【0043】

以上のように、本実施の形態1による公開鍵生成装置によれば、公開鍵生成装置15を、乱数生成手段11と公開鍵生成手段12とを1つのLSI15に集積

化して構成するようにしたので、従来、何ら安全対策のなされていない演算アルゴリズムを用いて秘密鍵及び共有鍵を作製する場合に比べて、秘密鍵 k_a は、チップ内部で公開鍵 y_a の生成にのみ用いられる構成となり、公開鍵生成装置 15 の数 1 式の演算が外部には漏れることがなく、このような LSI 13 を用いることで、本公開鍵生成装置 15 を公開鍵 y_a の生成以外に流用、あるいは改変することが極めて困難な状態となり、第 3 者の不正な攻撃に対する強度が極めて高い。

【0044】

なお、数 1 式に基づいて公開鍵 y_a を演算する例について説明したが、楕円曲線暗号を使用し、数 5 式に基づいて公開鍵 y_a を演算するようにしても、同様の効果が得られる。

【0045】

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

【0046】

(実施の形態 2)

次に、本発明の請求項 5 に対応する実施の形態 2 による共有鍵生成装置について説明する。

図 2 は、本発明の実施の形態 2 による共有鍵生成装置のブロック構成図を示すものである。図 2 において、図 1 と同一符号は同一、または相当部分を示し、21 は共有鍵生成手段、22 は乱数生成手段 11 と上記共有鍵生成手段 21 とを含む LSI、23 は LSI 22 を制御する制御手段、24 は共有鍵配布先となるユーザー 2 が生成した公開鍵を元に共有鍵を作成する、共有鍵配布元であるユーザー 1 の共有鍵生成装置を示す。以下、図 2 を参照しながら、本実施の形態 2 の共有鍵生成装置 24 の動作について説明する。

【0047】

乱数生成手段 11 は制御手段 23 に制御され、乱数 k_a を生成し、これを秘密鍵 k_a とする。ここで秘密鍵 k_a は、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とした時、 $0 < k_a < q$ を満たしている。制御手段 2

3は乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段23には、例えばマイクロコンピュータが使用される。さらに制御手段23は、共有鍵配布先となるユーザー2より数2式で表されるユーザー2の公開鍵 y_b を取得する。共有鍵生成手段21は制御手段23に制御され、共有鍵 K_a を生成する。共有鍵 K_a は数3式に基づいてユーザー1の秘密鍵 k_a とユーザー2の公開鍵 y_b とにより演算される。生成された共有鍵 K_a は、例えば、制御手段14によって秘密鍵暗号方式の鍵として用いられ、ユーザー1とユーザー2との間でこの共通の共有鍵 K_a を用いた暗号化伝送に使用される。

【0048】

以上の構成において、少なくとも乱数生成手段11と共有鍵生成手段21とをLSI22内部に集積すれば、数3式の演算を他の暗号処理へ流用あるいは改変することは非常に困難である。加えて制御手段23を集積すれば、さらに効果が高まる。また共有鍵 K_a 生成後、乱数生成手段11が新たに乱数を生成するようになれば、共有鍵 K_a は出力される毎に異なる値をとる。この時、数3式から明らかなように、共有鍵 K_a は乱数の関数となる。よって、ユーザー1を含めた誰もが本共有鍵生成装置24を共有鍵 K_a の生成以外に流用あるいは改変することは極めて困難である。

【0049】

以上のように、本実施の形態2による共有鍵生成装置によれば、共有鍵生成装置24を、乱数生成手段11と共有鍵生成手段21とを1つのLSI22に集積化して構成するようにしたので、秘密鍵 k_a はチップ内部で共有鍵 K_a の生成にのみ用いられる構成となり、共有鍵生成装置24の数3式の演算が外部には漏れることがなく、このようなLSI22を用いることで、本共有鍵生成装置24を共有鍵 K_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第三者の不正な攻撃に対する強度が極めて高い。

【0050】

なお、数3式に基づいて共有鍵 K_a を演算する例について説明したが、楕円曲線暗号を使用し、数7式に基づいて共有鍵 K_a を演算しても同様の効果が得られる。

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

【0051】

(実施の形態3)

次に、本発明の請求項9に対応する実施の形態3による鍵交換装置について説明する。

図3は、本発明の実施の形態3である鍵交換装置のブロック構成図を示すものである。

【0052】

図3において、図1または図2と同一符号は同一、または相当部分を示し、31は乱数生成手段11、公開鍵生成手段12、共有鍵生成手段21とを含むLSI、32はLSI31を制御する制御手段、33は公開鍵配布元、及び共有鍵配布先となるユーザー2の生成した公開鍵を基に作成した共有鍵の配布元、となるユーザー1の鍵交換装置である。

【0053】

以下、図3を参照しながら、実施の形態3の鍵交換装置の動作について説明する。

乱数生成手段11は制御手段32に制御され、乱数 k_a を生成し、これを秘密鍵 k_a とする。ここで秘密鍵 k_a は、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とした時、 $0 < k_a < q$ を満たしている。制御手段32は乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段32には、例えばマイクロコンピュータが使用される。公開鍵生成手段12は制御手段32に制御され、公開鍵 y_a を生成する。公開鍵 y_a は数1式に基づいて演算される。生成された公開鍵 y_a は、制御手段32によってユーザー2へ伝送される。

【0054】

さらに制御手段32は、ユーザー2より数2式で表されるユーザー2の公開鍵 y_b を取得する。共有鍵生成手段21は制御手段32に制御され、共有鍵 K_a を生成する。共有鍵 K_a は数3式に基づいて秘密鍵 k_a と公開鍵 y_b より演算され

る。生成された共有鍵 K_a は、制御手段 32 によって例えば秘密鍵暗号方式の鍵として用いられ、ユーザー 1 とユーザー 2 との間の暗号化伝送に使用される。

【0055】

少なくとも乱数生成手段 11 と公開鍵生成手段 12 と共有鍵生成手段 21 を LSI 31 内部に集積すれば、数 1 式および数 3 式の演算を他の暗号処理へ流用あるいは改変することは非常に困難である。加えて制御手段 32 を集積すれば、さらに効果が高まる。また公開鍵 y_a と共有鍵 K_a とを生成後、乱数生成手段 11 が新たに乱数を生成するようにすれば、数 1 式および数 3 式から明らかなように、公開鍵 y_a と共有鍵 K_a は乱数の関数となる。よって、ユーザー 1 を含めた誰もが本鍵交換装置 33 を鍵交換処理以外に流用あるいは改変することは極めて困難である。

【0056】

以上のように、本実施の形態 3 による鍵交換装置によれば、鍵交換装置 33 を、乱数生成手段 11 と公開鍵生成手段 12 と共有鍵生成手段 21 とを、1 つの LSI 131 に集積化して構成するようにしたので、秘密鍵 k_a はチップ内部で公開鍵 y_a 、及び共有鍵 K_a の生成にのみ用いられる構成となり、鍵交換装置 33 の数 1 式及び数 3 式の演算が外部には漏れることがなく、このような LSI 131 を用いることで本鍵交換装置 33 を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第 3 者の不正な攻撃に対する強度が極めて高い。

【0057】

なお、数 1 式および数 3 式に基づいて公開鍵 y_a と共有鍵 K_a を演算する例について説明したが、楕円曲線暗号を使用し、数 5 式および数 7 式に基づいて公開鍵 y_a と共有鍵 K_a とを演算しても同様の効果が得られる。

【0058】

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

なお、本実施の形態 3 における鍵交換装置 33 と同様の構成をもつ鍵交換装置をユーザー 2 が使用することによって、ユーザー 1 とユーザー 2 の間の鍵交換処

理を極めて安全に行うことができることは説明するまでもない。

【0059】

(実施の形態4)

次に、本発明の請求項13に対応する実施の形態4による鍵交換装置について説明する。

図4は、本発明の実施の形態4による鍵交換装置のブロック構成図を示すものである。

【0060】

図4において、図1または図2と同一符号は同一、または相当部分を示し、41は秘密鍵保持手段、42は乱数生成手段11、公開鍵生成手段、共有鍵生成手段21、秘密鍵保持手段41とを含むLSI、43はLSI42を制御する制御手段、44は公開鍵配布元、及び共有鍵配布先となるユーザー2の生成した公開鍵を基に作成した共有鍵の配布元、となるユーザー1の鍵交換装置である。以下、図4を参照しながら、本実施の形態4の鍵交換装置の動作について説明する。

【0061】

乱数生成手段11は制御手段43に制御され、乱数 k_a を生成し、これを秘密鍵 k_a とする。ここで秘密鍵 k_a は、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とした時、 $0 < k_a < q$ を満たしている。制御手段43は乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段43には、例えばマイクロコンピュータが使用される。秘密鍵保持手段41は秘密鍵 k_a を一時的に記憶する。公開鍵生成手段12は制御手段43に制御され、公開鍵 y_a を生成する。公開鍵 y_a は数1式に基づいて演算される。生成された公開鍵 y_a は、制御手段43によってユーザー2へ伝送される。

【0062】

さらに制御手段43は、ユーザー2より数2式で表されるユーザー2の公開鍵 y_b を取得する。共有鍵生成手段21は制御手段43に制御され、共有鍵 K_a を生成する。共有鍵 K_a は数3式に基づいて秘密鍵保持手段41が記憶している秘密鍵 k_a と公開鍵 y_b とより演算される。生成された共有鍵 K_a は、制御手段43によって、例えば秘密鍵暗号方式の鍵として用いられ、ユーザー1とユーザー

2 との間の暗号化伝送に使用される。

【0063】

少なくとも乱数生成手段 11 と公開鍵生成手段 12 と共有鍵生成手段 21 と秘密鍵保持手段 41 とを LSI 42 内部に集積すれば、数 1 式および数 3 式の演算を他の暗号処理へ流用あるいは改変することは非常に困難である。加えて制御手段 43 を集積すれば、さらに効果が高まる。

【0064】

また公開鍵 y_a を生成後、乱数生成手段 11 が新たに乱数を生成するようにすれば、公開鍵 y_a は出力される毎に異なる値をとる。この時、数 1 式から明らかなように、公開鍵 y_a は乱数の関数となる。共有鍵生成手段 21 が共有鍵 K_a を生成する以前に、乱数生成手段 11 が新たに乱数を生成しても、秘密鍵保持手段 41 が秘密鍵 k_a を保持しているため、共有鍵生成手段 21 は正しく共有鍵 K_a を生成することができる。

【0065】

加えて、共有鍵生成手段 21 により共有鍵 K_a を生成した後、乱数生成手段 11 が新たに乱数を生成し、生成した乱数を秘密鍵保持手段 41 が保持するようにすれば、共有鍵 K_a は出力される毎に異なる値をとる。この時、数 3 式から明らかなように、共有鍵 K_a は乱数の関数となる。

【0066】

よって、ユーザー 1 を含めた誰もが本鍵交換装置を鍵交換処理以外に流用あるいは改変することは極めて困難である。また LSI 42 の外部に出力される公開鍵 y_a 、共有鍵 K_a を観測しても乱数の関数となっているため、公開鍵生成手段 12 と共有鍵生成手段 21 の構成を類推することすら不可能である。

【0067】

以上のように、本実施の形態 4 による鍵交換装置によれば、鍵交換装置 44 を、乱数生成手段 11 と公開鍵生成手段 12 と共有鍵生成手段 21 と秘密鍵保持手段 41 とを 1 つの LSI 42 に集積化して構成するようにしたので、秘密鍵 k_a はチップ内部で公開鍵 y_a 、及び共有鍵 K_a の生成にのみ用いられる構成となり、鍵交換装置 44 の数 1 式及び数 3 式の演算が外部には漏れることがなく、この

ようなLSI42を用いることで本鍵交換装置44を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第3者の不正な攻撃に対する強度が極めて高い。

【0068】

加えて、共有鍵生成手段21が共有鍵 K_a を生成する以前に、乱数生成手段11が新たに乱数を生成しても、共有鍵生成手段21が正しく共有鍵 K_a を生成することができる。

【0069】

なお、数1式および数3式に基づいて公開鍵 y_a と共有鍵 K_a を演算する例について説明したが、楕円曲線暗号を使用し、数5式および数7式に基づいて公開鍵 y_a と共有鍵 K_a を演算しても同様の効果が得られる。

【0070】

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

【0071】

なお、本実施の形態4における鍵交換装置44と同様の構成をもつ鍵交換装置をユーザー2が使用することによって、ユーザー1とユーザー2の間の鍵交換処理を極めて安全に行うことができることは説明するまでもない。

【0072】

【発明の効果】

以上のように、本発明の請求項1にかかる公開鍵生成装置によれば、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、前記乱数 k_a と、前記元 g と、前記素数 q より、公開鍵 y_a を前記有限群 F 上で演算し出力する公開鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段とが同一の半導体集積回路上に集積され、公開鍵配布元となる第1のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y_a を取得し、該公開鍵 y_a を公開鍵配布先となる第2のユーザーへ伝送するものとしたので、秘密鍵 k_a は半導体集積回路のチップ内部で公開鍵 y_a の生成にのみ用いられる構成とな

り、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本公開鍵生成装置を公開鍵 y_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0073】

また、本発明の請求項2にかかる公開鍵生成装置によれば、請求項1記載の公開鍵生成装置において、前記公開鍵生成手段は、前記乱数 k_a と、前記元 g と、前記素数 q より、前記公開鍵 y_a を、 $y_a = g^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力するものとしたので、有限群 F における離散対数問題の解法の困難性を根拠とした暗号系において、公開鍵生成装置を公開鍵 y_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0074】

また、本発明の請求項3にかかる公開鍵生成装置によれば、請求項1記載の公開鍵生成装置において、前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記公開鍵生成手段が、前記乱数 k_a と、前記元 G と、前記素数 q より、前記公開鍵 y_a を、 $y_a = k_a G \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力するものとしたので、楕円曲線暗号系においても、公開鍵生成装置を公開鍵 y_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0075】

また、本発明の請求項4にかかる公開鍵生成装置によれば、請求項1ないし3のいずれかに記載の公開鍵生成装置において、前記乱数生成手段が、前記公開鍵 y_a の演算終了後に、新たな乱数を生成するものとしたので、公開鍵 y_a は出力される毎に異なるものとなり、第3者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【0076】

また、本発明の請求項5にかかる共有鍵生成装置は、乗算が定義された有限群

F上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、共有鍵配布先となる第2のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記乱数 k_a より、共有鍵 K_a を前記有限群 F 上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第1のユーザーの制御手段が、前記共有鍵配布先となる第2のユーザーより前記公開鍵 y_b を取得し、前記乱数生成手段と前記共有鍵生成手段とを制御して、前記共有鍵 K_a を導出するものとしたので、秘密鍵 k_a は半導体集積回路のチップ内部で共有鍵 K_a の生成にのみ用いられる構成となり、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本共有鍵生成装置を共有鍵 K_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0077】

また、本発明の請求項6にかかる共有鍵生成装置は、請求項5記載の共有鍵生成装置において、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、 $K_a = y_b^{k_a} \bmod q$ として、前記有限群 F 上で演算し出力するものとしたので、有限群 F における離散対数問題の解法の困難性を根拠とした暗号系において、共有鍵生成装置を共有鍵 K_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0078】

また、本発明の請求項7にかかる共有鍵生成装置は、請求項5記載の共有鍵生成装置において、前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが前記乱数 k_b より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y_b = k_b G \bmod q$ と、前記乱数 k_a により、前記共有鍵 K_a を、 $K_a = k_a y_b \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力するも

のとしたので、楕円曲線暗号系においても、共有鍵生成装置を共有鍵 K_a の生成以外に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0079】

また、本発明の請求項8にかかる共有鍵生成装置は、請求項5ないし7のいずれかに記載の共有鍵生成装置において、前記乱数生成手段は、前記共有鍵 K_a の演算終了後に、新たな乱数を生成するものとしたので、共有鍵 K_a は出力される毎に異なるものとなり、第3者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【0080】

また、本発明の請求項9にかかる鍵交換装置は、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、前記乱数 k_a と、前記元 g と、前記素数 q より、公開鍵 y_a を前記有限群 F 上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第2のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記乱数 k_a より、共有鍵 K_a を前記有限群 F 上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第1のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y_b を取得し、前記共有鍵生成手段を制御して前記共有鍵 K_a を導出するものとしたので、秘密鍵 k_a は半導体集積回路のチップ内部で公開鍵 y_a 、及び共有鍵 K_a の生成にのみ用いられる構成となり、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第3者の不正な攻撃に対する強度が極めて高いものとすることができるという効果が得られる。

【0081】

また、本発明の請求項10にかかる鍵交換装置は、請求項9記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数 k_a と、前記元 g と、前記素数 q よ

り、前記公開鍵 $y a$ を $y a = g^{k a} \bmod q$ として、前記有限群 F 上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第 2 のユーザーが、前記乱数 $k b$ より前記有限群 F 上で演算し生成した前記公開鍵 $y b = g^{k b} \bmod q$ と、前記乱数 $k a$ により、前記共有鍵 $K a$ を $K a = y b^{k a} \bmod q$ として、前記有限群 F 上で演算し出力するものとしたので、有限群 F における離散対数問題の解法の困難性を根拠とした暗号系において、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第 3 者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0082】

また、本発明の請求項 11 にかかる鍵交換装置は、請求項 9 記載の鍵交換装置において、前記有限群 F を有限体上の楕円曲線 $E(F)$ とし、前記楕円曲線 $E(F)$ の元を G とし、前記公開鍵生成手段は、前記乱数 $k a$ と、前記元 G と、前記素数 q より、前記公開鍵 $y a$ を、 $y a = k a G \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる前記第 2 のユーザーが、前記乱数 $k b$ より前記楕円曲線 $E(F)$ 上で演算し生成した前記公開鍵 $y b = k b G \bmod q$ と、前記乱数 $k a$ により、前記共有鍵 $K a$ を、 $K a = k a y b \bmod q$ として、前記楕円曲線 $E(F)$ 上で演算し出力するものとしたので、楕円曲線暗号系においても、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第 3 者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0083】

また、本発明の請求項 12 にかかる鍵交換装置は、請求項 9 ないし 11 のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵 $y a$ と前記共有鍵 $K a$ の演算がともに終了した後に、新たな乱数を生成するものとしたので、公開鍵 $y a$ 、及び共有鍵 $K a$ は出力される毎に異なるものとなり、第 3 者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【0084】

また、本発明の請求項13にかかる鍵交換装置は、乗算が定義された有限群F上の元をg、前記gの素数である位数をqとし、 $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段と、前記乱数 k_a を一時的に記憶する秘密鍵保持手段と、前記乱数 k_a と、前記元gと、前記素数qより、公開鍵 y_a を前記有限群F上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第2のユーザーが発生した $0 < k_b < q$ となる乱数 k_b より生成された公開鍵 y_b と、前記秘密鍵保持手段が保持する乱数 k_a により、共有鍵 K_a を前記有限群F上で演算し出力する共有鍵生成手段とを備え、少なくとも、前記乱数生成手段と、前記秘密鍵保持手段と、前記公開鍵生成手段と、前記共有鍵生成手段とが、同一の半導体集積回路上に集積され、共有鍵配布元となる第1のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵 y_a を取得して、該公開鍵 y_a を前記共有鍵配布先となる第2のユーザーへ伝送し、前記共有鍵配布先となる第2のユーザーより前記公開鍵 y_b を取得して、前記共有鍵生成手段を制御して前記共有鍵 K_a を導出するものとしたので、秘密鍵 k_a は半導体集積回路のチップ内部で公開鍵 y_a 、及び共有鍵 K_a の生成にのみ用いられる構成となり、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第3者の不正な攻撃に対する強度が極めて高いものとすることができるという効果が得られるのに加えて、共有鍵生成手段が共有鍵 K_a を生成する以前に、乱数生成手段が新たに乱数を生成しても、共有鍵生成手段は正しく共有鍵 K_a を生成することができるという効果が得られる。

【0085】

また、本発明の請求項14にかかる鍵交換装置は、請求項13記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数 k_a と前記元gと前記素数qより前記公開鍵 y_a を、 $y_a = g^{k_a} \bmod q$ として、前記有限群F上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが前記乱数 k_b より前記有限群F上で演算し生成した前記公開鍵 $y_b = g^{k_b} \bmod q$ と前記秘密鍵保持手段が記憶している乱数 k_a より前記共有鍵 K_a を、

$Ka = yb \cdot ka \bmod q$ として、前記有限群F上で演算し出力するものとしたので、有限群Fにおける離散対数問題の解法の困難性を根拠とした暗号系において、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0086】

また、本発明の請求項15にかかる鍵交換装置は、請求項13記載の鍵交換装置において、前記有限群Fを有限体上の楕円曲線E(F)とし、前記楕円曲線E(F)の元をGとし、前記公開鍵生成手段は、前記乱数kaと、前記元Gと、前記素数qより、前記公開鍵yaを、 $ya = kaG \bmod q$ として、前記楕円曲線E(F)上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第2のユーザーが、前記乱数kbより前記楕円曲線E(F)上で演算し生成した前記公開鍵yb= $kbG \bmod q$ と、前記秘密鍵保持手段が記憶している乱数kaにより、前記共有鍵Kaを、 $Ka = kayb \bmod q$ として、前記楕円曲線E(F)上で演算し出力するものとしたので、楕円曲線暗号系においても、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第3者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【0087】

また、本発明の請求項16にかかる鍵交換装置は、請求項13ないし15のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵yaの演算終了後に、新たな乱数を生成するようにしたので、公開鍵ya、及び共有鍵Kaは出力される毎に異なるものとなり、第3者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【0088】

また、本発明の請求項17にかかる鍵交換装置は、請求項13ないし15のいずれかに記載の鍵交換装置において、

【0089】

前記乱数生成手段は、前記共有鍵Kaの演算終了後に、新たな乱数を生成し、

前記秘密鍵保持手段が、前記乱数生成手段の生成した前記新たな乱数を保持するようにしたので、共有鍵生成手段が共有鍵 K a を生成する以前に、乱数生成手段が新たに乱数を生成しても、共有鍵生成手段が正しく共有鍵 K a を生成することができるという効果が得られる。

【0090】

また、本発明の請求項 1 8 にかかる鍵交換方法は、請求項 9 ないし 1 7 のいずれかに記載の鍵交換装置を使用し、鍵を共有したいユーザーの双方が前記鍵を共有するようにしたので、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで暗号鍵生成、または鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第 3 者の不正な攻撃に対する強度が極めて高いものとすることができるという効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における公開鍵生成装置の構成を示すブロック構成図である。

【図 2】

本発明の実施の形態 2 における共有鍵生成装置の構成を示すブロック構成図である。

【図 3】

本発明の実施の形態 3 における鍵交換装置の構成を示すブロック構成図である。

【図 4】

本発明の実施の形態 4 における鍵交換装置の構成を示すブロック構成図である。

【図 5】

従来の鍵交換装置の構成を示すブロック構成図である。

【符号の説明】

- 1 1 乱数生成手段
- 1 2 公開鍵生成手段

1 3, 2 2, 3 1, 4 2 L S I

1 4, 2 3, 3 2, 4 3 制御手段

1 5 公開鍵生成装置

2 1 共有鍵生成手段

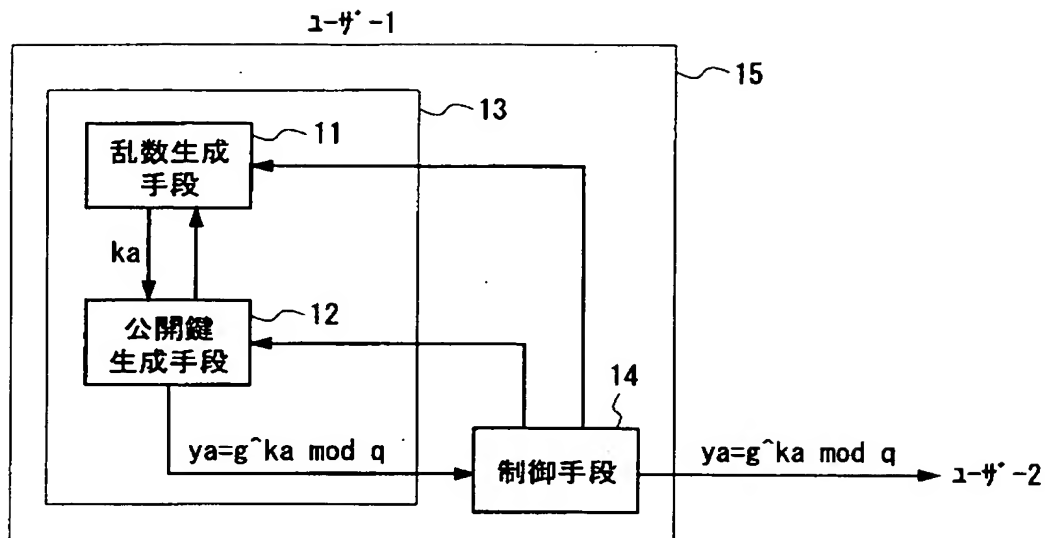
2 4 共有鍵生成装置

3 3, 4 4 鍵交換装置

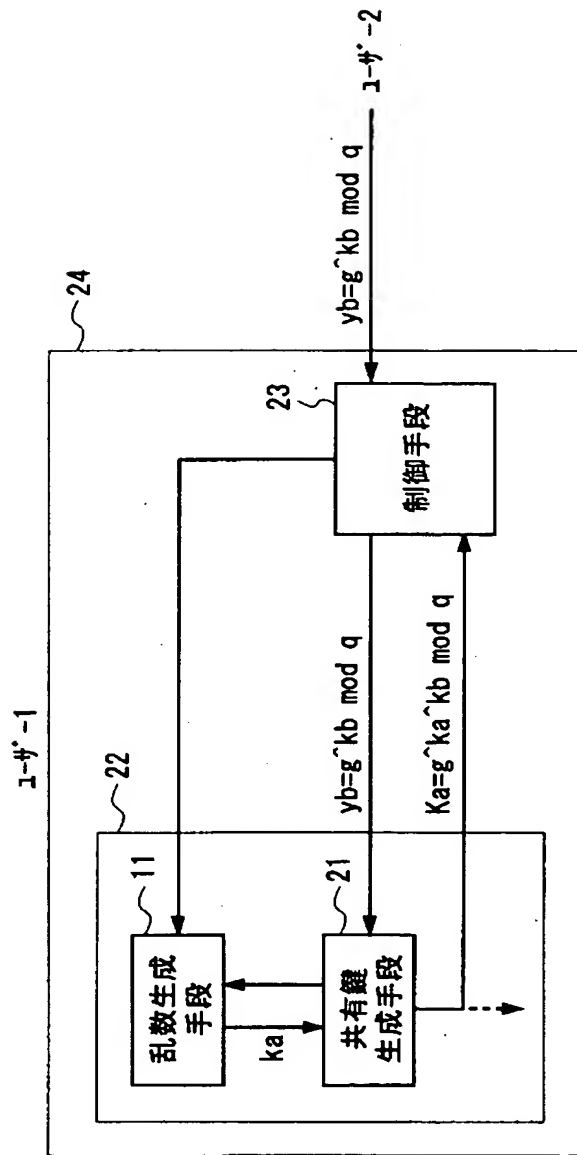
4 1 秘密鍵保持手段

【書類名】 図面

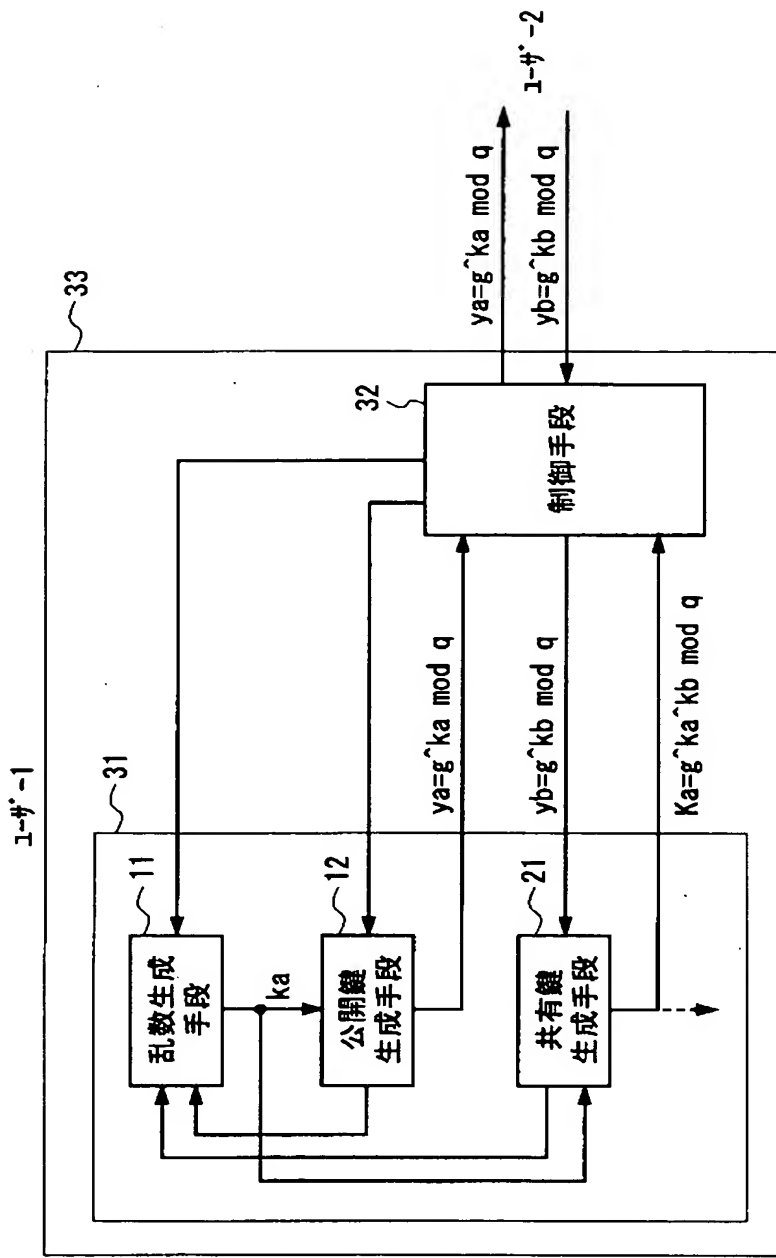
【図 1】



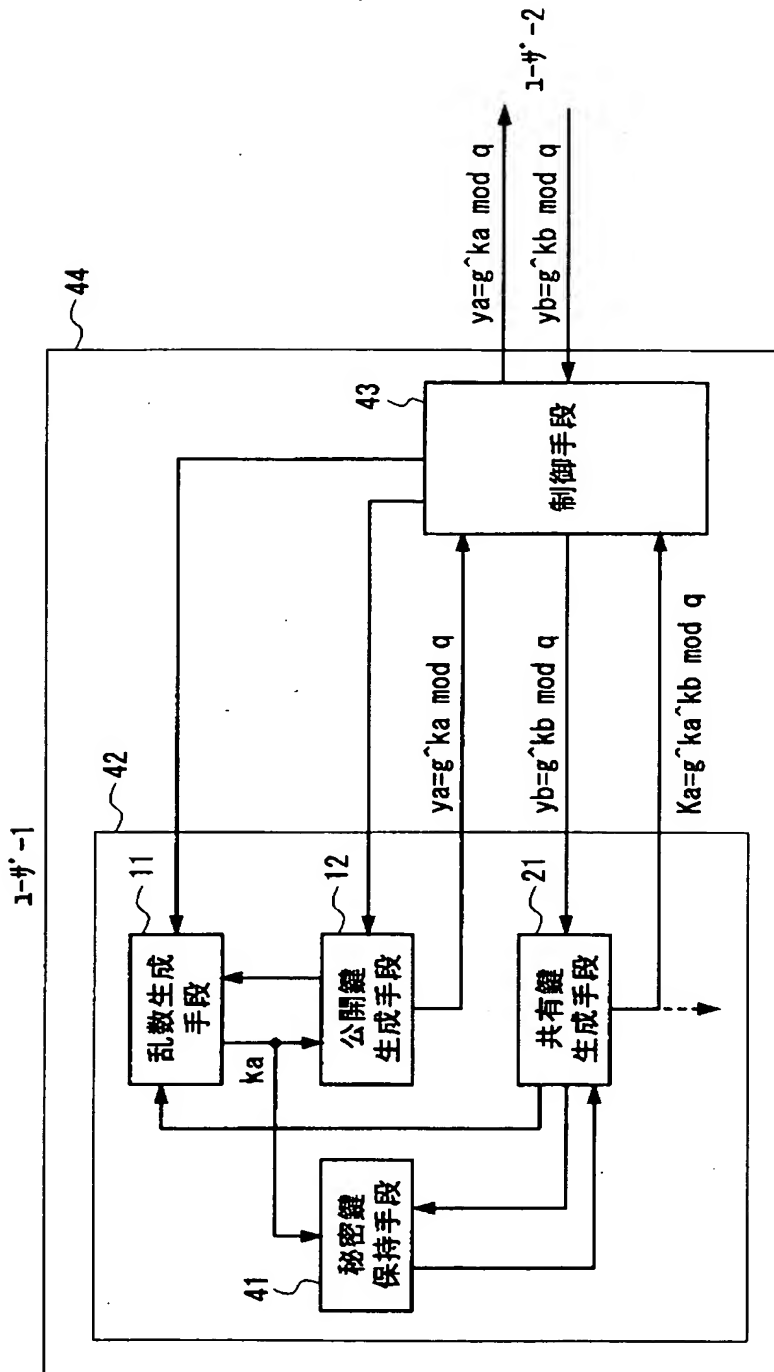
【図 2】



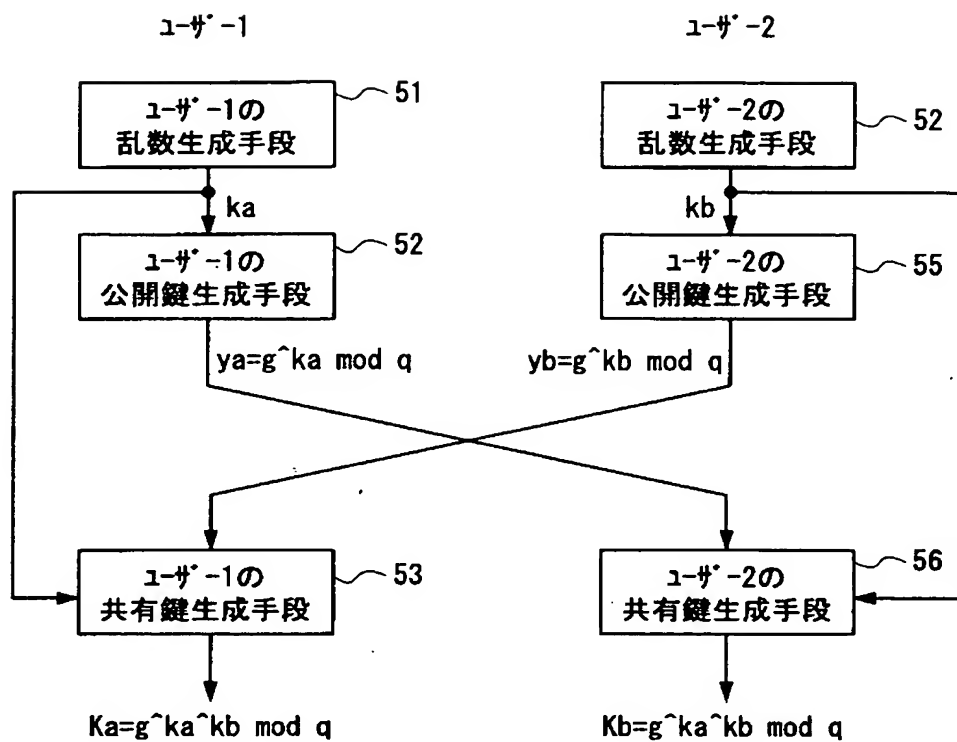
【図 3】



【図 4】



【図5】



【書類名】 要約書

【要約】

【課題】 DH鍵交換処理時の鍵演算処理を第3者から秘匿し、第3者による装置の流用あるいは改変が極めて困難な公開鍵生成装置、共有鍵生成装置、鍵交換装置及び鍵交換方法を提供すること。

【解決手段】 公開鍵生成装置 1 5 を、乗算が定義された有限群 F 上の元を g 、前記 g の素数である位数を q とし $0 < k_a < q$ となる乱数 k_a を生成する乱数生成手段 1 1、及び前記乱数 k_a と前記元 g と前記素数 q より公開鍵 y_a を前記有限群 F 上で演算し出力する公開鍵生成手段 1 2 を 1 つの L S I 1 5 に集積化し、秘密鍵 k_a がチップ内部で公開鍵 y_a の生成にのみ用いられる構成とし、公開鍵生成装置 1 5 の暗号化演算が外部に漏れないようにする。

【選択図】 図 3

特願 2003-088788

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社